APLIKASI CHATTING PADA JARINGAN MANET DENGAN FITUR ENKRIPSI MENGGUNAKAN NACL

Oleh:
Agus Wijanarko
NIM: 622013012

Skripsi
Untuk melengkapi salah satu syarat memperoleh
Gelar Sarjana Teknik
Program Studi Sistem Komputer
Fakultas Teknik Elektronika dan Komputer
Universitas Kristen Satya Wacana Salatiga

Juli 2018

APLIKASI CHATTING PADA JARINGAN MANET
DENGAN FITUR ENKRIPSI MENGGUNAKAN NACL

Oleh:
Agus Wijanarko
NIM: 622013012

Skripsi ini telah diterima dan disahkan
Untuk melengkapi salah satu syarat memperoleh
Gelar Sarjana Teknik
dalam
Program Studi Sistem Komputer
Fakultas Teknik Elektronika Dan Komputer
Universitas Kristen Satya Wacana
Salatiga

Disahkan Oleh

Pembimbing I	Pembimbing II
Banu Wirawan Yohanes, M.CompSc.	Hartanto Kusuma Wardana, M.T
Tgl. 31 Juli 2018	Tgl. 31 Juli 2018

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : Agus Wijanarko

NIM : 622013012 Email : 622013012@student.uksw.edu

Fakultas : FTEK Program Studi : Sistem Komputer

Judul tugas akhir : Aplikasi Chatting pada Jaringan MANET
Dengan Fitur Enkripsi Menggunakan NaCl

Pembimbing : 1. Banu Wirawan Yohanes , M.CompSc
2. Hartanato Kusuma Wardana, M.T

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 1 Agustus 2018

(Agus Wijanarko)

F-LIB-080

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Agus Wijanarko

NIM : 622013012 Email : 622013012@student.uksw.edu

Fakultas : FTEK Program Studi : Sistem Komputer

Judul tugas akhir : Aplikasi Chatting pada Jaringan MANET
Dengan Fitur Enkripsi Menggunakan NaCl

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☐ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☑ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-ekslusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 18 Juli 2018

Agus Wijanarko

Tanda tangan & nama terang mahasiswa

Mengetahui,

Banu W. Yohanes

Tanda tangan & nama terang pembimbing I

Hartanto

Tanda tangan & nama terang pembimbing II

INTISARI

Dengan banyaknya perangkat *mobile*, kegiatan mobilitas pun semakin meningkat. Namun mengingat jaringan internet pada wilayah Indonesia belum merata dan stabil, penggunaan WLAN dapat menjadi solusi permasalahan. Namun WLAN itu sendiri sangat rawan karena setiap pengguna dapat dengan mudah terhubung dengan jaringan jika berada dalam jangkauan WLAN tersebut. Perlu ditambahkan sebuah sistem untuk mengamankan dan menjamin kerahasian dari data yang dipertukarkan.

Skripsi ini berisi tentang pembuatan sebuah aplikasi chatting dengan menerapkan MANET dan fungsi enkripsi kunci publik yang terdapat dalam NaCl. Raspberry Pi digunakan sebagai *node* untuk menjalankan sistem yang dibuat. Setiap *node* akan menjalankan konfigurasi MANET, NaCl, *database*, sinkronisasi kontak dan chat. Konfigurasi MANET adalah sebuah konfigurasi yang terdiri dari *ad-hoc* dan OLSRd yang digunakan untuk membangun jaringan MANET. Sistem akan menjalankan sinkronisasi kontak untuk pembuatan akun dan kemudian berjalan pada *background* untuk melakukan *update* kontak list. Proses sinkronisasi kontak ini akan disertai dengan NaCl untuk pembangkitan kunci dan *database*. Proses chat adalah proses yang terdiri dari *thread* kirim dan terima yang digunakan untuk chatting. Proses chat ini disertai dengan NaCl untuk proses enkripsi dekripsi serta *database* untuk proses menyimpan dan menggambil data.

Implementasi MANET dan NaCl menghasilkan topologi jaringan yang dinamis dan terdapat jaminan kerahasian data. Pada MANET topologi akan berubah jika ada perubahan pada jumlah *node*. Proses komunikasi antar *node* berjalan lancar baik chatting maupun pertukaran data user. MANET yang dibangun dengan tiga buah *node* dapat digunakan untuk memanipulasi jumlah hop, sehingga dapat diukur waktunya untuk jumlah n-hop. Pengukuran juga dilakukan untuk mengetahui performa dari sistem yang dibuat.

ABSTRACT

With so many mobile devices, mobility activities are increasing. However, given the internet network in Indonesia is not evenly distributed and stable, the use of WLAN can be a solution to the problem. But the WLAN itself is very vulnerable because each user can easily connect to the network if it is within range of the WLAN. It is necessary to add a system to secure and ensure the confidentiality of data exchanged

This thesis is about making a chat application by applying MANET and public key encryption function contained in NaCl. Raspberry Pi is used as the node to run the created system. Each node will run MANET, NaCl, database configuration, contact sync and chat. The MANET configuration is a configuration consisting of ad-hoc and OLSRd used to build the MANET network. The system will run a contact synchronization for account creation and then run in the background to update contact list. This contact synchronization process will be accompanied by NaCl for key generation and database. The chat process is a process consisting of a thread of send and receive used for chatting. This chat process is accompanied by NaCl for the process of encrypting the decryption and database for the process of storing and retrieving data.

MANET and NaCl implementations produce a dynamic network topology and there is a guarantee of data confidentiality. In the MANET topology will change if there is a change in the number of nodes. Communication process between nodes run smoothly both chat and exchange data user. MANETs built with three nodes can be used to manipulate the number of hops, so it can be timed for the number of n-hops. Measurements are also performed to determine the performance of the system created.

KATA PENGANTAR

Puji dan syukur kepada Tuhan yang Maha Esa, karena atas limpahan berkat dan rahmat-Nya penulis mampu menyelesaikan skripsi ini sebagai syarat untuk menyelesaikan studi pada Fakultas Teknik Elektronika dan Komputer Universitas Kristen Satya Wacana. Dalam proses penyusunan dan penyelesaian skripsi ini, penulis mendapatkan bantuan dari orang-orang di sekitar. Oleh karena itu, penulis ingin mengucapkAn terimakasih kepada:

1. Bapak Banu Wirawan Yohanes, M.CompSc dan Bapak Hartanto Kusuma W, M.T selaku pembimbing atas bimbingan, saran, serta nasehat yang telah diberikan selama proses pembuatan skripsi.
2. Bapak Darmawan Utomo, M.Eng selaku wali studi atas arahan serta nasehat yang telah diberikan selama berkuliah di Fakultas Elektronika dan Komputer Universitas Kristen Satya Wacana.
3. Seluruh dosen atas ilmu yang telah diberikan selama berkuliah di Universitas Kristen Satya Wacana.
4. Kedua orang tua serta seluruh keluarga atas dukungan berupa dukungan moral, doa serta materiil yang telah diberikan kepada penulis.
5. Teman-teman dan sahabat seperjuangan FTEK angkatan 2013 yang telah menemani, memberikan doa, motivasi serta memberikan saran kepada penulis.
6. Seluruh karyawan Tata Usaha yang telah membantu kelancaran penyelesaian pembuatan skripsi ini.
7. Seluruh pihak yang membantu penulis selama proses pembuatan skripsi yang tidak dapat disebutkan satu per satu.

Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan baik dalam isi, penyampaian, serta penulisan. Sehingga, dibutuhkan kritik dan saran yang membangun demi perbaikan skripsi ini ke depannya.

Salatiga, 2 Juli 2018

Penulis,

Agus Wijanarko

DAFTAR ISI

INTISARI i

ABSTRACT ii

KATA PENGANTAR iii

DAFTAR ISI iv

DAFTAR GAMBAR vii

DAFTAR TABEL x

DAFTAR KODE xi

DAFTAR SINGKATAN xii

BAB I PENDAHULUAN 1

1.1. Tujuan 1

1.2. Latar Belakang 1

1.3. Gambaran Sistem 2

1.4. Spesifikasi Sistem 4

1.5. Sistematika Penulisan 5

BAB II DASAR TEORI 6

2.1. Raspberry Pi 6

2.2. Python 7

2.3. IEEE 802.11 7

2.4. Mobile Ad-hoc Network 8

2.5. Optimized Link Stated Routing (RFC 3626) 9

2.6. MySQL 12

2.7. NaCl 12

BAB III PERANCANGAN 17
3.1. Arsitektur Sistem 17
3.2. Node 18
3.2.1. Instalasi *Node* 19
3.2.2. Konfigurasi Mysql 20
3.3. MANET 23
3.3.1. *Ad-hoc mesh* 24
3.3.2. OLSRd 25
3.4. Sinkronisasi kontak 25
3.4.1. Membuat Akun 26
3.4.2. Pasif *Thread* 28
3.4.3. Aktif *Thread* 29
3.5. Chat 30
3.5.1. Terima Pesan 31
3.5.2. Kirim Pesan 32
3.5.3. Komunikasi Grup 34
3.6. NaCl 35
3.6.1. Protokol Enkripsi Kunci Publik 35
3.6.2. Pembangkitan Kunci NaCl 39
3.6.3. Enkripsi Kunci Publik NaCl 39
3.6.4. Dekripsi Kunci Publik NaCl 42
3.7. Database 44
3.7.1. Ambil Data 44
3.7.2. Input Data 45

BAB IV PENGUJIAN DAN ANALISIS 47
4.1. Jaringan MANET 47
4.1.1. Membangun Jaringan MANET 47
4.1.2. *Routing* MANET 49
4.2. Akun 51
4.2.1. Pembuatan Akun 51
4.2.2. Pertukaran Data Pengguna 54
4.3. Chatting 55
4.3.1. Privat chat 56
4.3.2. Grup chat 57
4.3.3. Pengukuran waktu pengirman pesan 59
4.4. NaCl 61
4.4.1. Enkripsi dan Dekripsi 61
4.4.2. Pengecekan Data Pesan dari *Database* 63
4.5. Performa Sistem 64
BAB V KESIMPULAN DAN SARAN 67
5.1. Kesimpulan 67
5.2. Saran 68
DAFTAR PUSTAKA 69